Cyber Threats to Employee Data and Other Confidential Information Are Front and Center in 2017

By Brian G. Cesaratto and Adam S. Forman

Now more than ever it is vitally important that employers institute personnel policies and technologies, train employees, and take other affirmative steps to protect against loss of employee personally identifiable information and other sensitive data from cyber threats. The authors of this article discuss the issue, recent litigation, and steps to take to avoid data breaches.

One need only look as far as recent headlines – where the presidential election and hacking received equal billing – to understand that technology's threats are escalating. The Democratic National Committee now joins a long list of companies in various industries that have been victims of hacking, including financial services and healthcare, among many. Risks to proprietary and confidential information, affecting millions of people, and the resulting public fallout annually escalate. The dramatic end to the 2016 election year foretells an even further increase in hacking events targeting companies and institutions of all sizes in 2017.

Companies must become even more vigilant to protect their employees' personally identifiable information ("PII") and assets. It is critically important that employers institute personnel policies and technologies, train employees and take other affirmative steps to protect against loss of employee PII and other sensitive data from cyber threats.

OF CONCERN TO GENERAL COUNSELS

Not surprisingly, these trends are increasingly concerning general counsels. A recent survey reports that 74 percent of corporate counsel named data breaches as their top data-related legal risk.[1] Another survey reports that 31 percent of general counsels identify data protection and cyber security protection as their top concern.[2] The "why" behind their legal worries is easily identified; just follow the daily news reporting of multiple high profile data breaches and the ensuing multi-million dollar settlements of class action claims. General counsels recognize that a data breach will, at a minimum, result in negative publicity and a loss of confidence in the organization. There will certainly be significant financial costs to mitigate the reputational harm and other fallout.

According to a recent IBM and Ponemon Institute study, a typical data breach costs a company just over $7 million.[3] Depending on the industry involved or the state where the breach occurred, there may be obligations to report the breach to the government or to the affected persons (including current and former employees), and respond to an ensuing governmental investigation.[4] Of course, class action lawsuits, damages claims and legal defense costs are sure to follow. A company's stock may also be negatively affected, or even targeted.[5] For example, one hedge fund has purportedly embarked on a conspicuous strategy to identify and publish alleged cyber security weaknesses while selling short the company's stock.[6]

The general counsels' concerns mount even further when considering that threats from employees can be just as serious as outside attackers, and that even an employee's careless or unknowing behavior can result in as damaging a breach as one due to malicious conduct. In particular, employees who are not aware of the dangers of social engineering attacks, such as phishing and spear-phishing, may inadvertently cause a significant data breach simply by responding to a fraudulent email. For example, the attacks on the Democratic National Committee reportedly involved successful phishing and spear phishing attacks using the organization's email systems.[7] Thus, the risks are real and growing, and the concerns well founded.

WHERE TO BEGIN?

A logical starting point for a comprehensive strategy to minimize those risks is to look at the nature of the claims asserted in the ever expanding litany of breach litigations. Most significantly, employees whose PII has been disclosed will allege that the company acted negligently by failing to take due care to protect confidential data from disclosure.[8] Numerous state laws also provide for private causes of action in the event of a data breach involving personal information, including employee PII, such as social security numbers and medical information.[9]

Affected employees are likely to claim that there was breach of an express or implied contract to protect the information arising out of the terms and conditions of employment. Failure to make timely notification to affected individuals or institutions may lead to additional statutory and common law claims.[10] Moreover, the failure to

provide timely notification of the breach (which if it had been made would presumably prompt remedial measures to avoid actual identity theft) may also increase the likelihood that employee-plaintiffs can later establish standing as courts have found standing to sue where the plaintiffs have suffered identity theft attacks.[11] Thus, breach related claims target both the inadequacy of preventative measures and the timeliness and sufficiency of the company's response should a breach occur.

LITIGATION

The litigations in Enslin v. Coca-Cola Company, Corona v. Sony Pictures and In Re U.S. Office of Personnel Management Data Security Breach Litigation are illustrative of the risks to employee PII that employers should address. The lead plaintiff in the Coca-Cola litigation was a former employee who brought a class action on behalf of 70,000 putative class members alleging statutory violations and common law claims grounded in negligence. Plaintiff claimed that 55 laptop computers containing employee PII, including social security numbers, financial and banking information, driver's license information and other sensitive material for over 70,000 current and former employees maintained by Coke's human resources department were stolen by another Coke employee.[12] The complaint pointed to the lack of encryption of the employee PII as one of the primary failures to institute adequate safeguards. The claims also included assertions that the failure to provide prompt notice of the thefts to employees was grossly negligent conduct "in the face of a preventable event."

It is interesting that in making their claims, employee-plaintiffs pointed to various standards of due care that were allegedly breached:

i. the Organization for Economic Cooperation and Development framework for security of computers and networks;
ii. the United States National Institute of Standards and Technology ("NIST") standards for securing information technology systems; and
iii. the Federal Trade Commission's guide to "Protecting Personal Information: A Guide for Business."

These standards of care were purportedly breached when employee PII was retained without business need, the PII was not protected through encryption or other controls, and there lacked sound destruction practices. Although the district court dismissed the state law negligence claims as barred under the economic loss doctrine, it recognized that there are exceptions that may in other cases permit negligence claims even where there are economic damages unaccompanied by physical injury or property damage (e.g., where the plaintiffs are able to show the existence of a special relationship to protect the information).[13]

Other courts have refused to dismiss negligence claims based on similar theories on a motion to dismiss.[14] Significantly, the district court in Enslin allowed the employees' contract claims to proceed premised on the asserted "promise of employment, with

salary, benefits and secure PHI" and to safeguard PII through "privacy policies, codes of conduct, and company security policies."[15]

In Corona, plaintiffs, all former employees of Sony, asserted claims including negligence, breach of implied contract, and violation of the California Confidentiality of Medical Information Act.[16] Plaintiffs alleged that as a result of inadequate security measures, Sony's network was hacked and that among the nearly 100 terabytes of data stolen was sensitive personal information of at least 15,000 current and former Sony employees. The information, which included employee financial, medical, and other PII, was purportedly used to threaten the individuals and their families, and was posted on the internet.

Plaintiffs claimed that they face ongoing future vulnerability to identity theft, medical theft, tax fraud, and financial theft because their PII has been, and may still be, publicly available to anyone with an internet connection, and their PII has already been traded on black market websites and used by identity thieves. Plaintiffs alleged that Sony failed to encrypt data and take other protection measures in accordance with "industry safeguards."

In denying Sony's motion to dismiss the claims of negligence and violations of the California Confidentiality of Medical Information Act, the court held that the employee-plaintiffs' allegations that they were required to provide PII to Sony in order to obtain compensation and employment benefits, and that the breach was foreseeable, established a special relationship providing an exception to the economic loss doctrine.

Similarly, the class action plaintiffs in In Re: U.S. Office of Personnel Management Data Security Breach Litigation, including employees, alleged that the OPM failed to safeguard their PII (e.g., birthdates, background check information, social security numbers, financial information, emotional health related information, private facts) asserting causes of action, inter alia, in negligence, negligent misrepresentation and concealment, invasion of privacy and breach of contract.[17]

Similar to the allegations in Corona, plaintiffs alleged that the employee-plaintiffs agreed to provide their sensitive personal information in exchange for the opportunity to be considered for employment and with assurances that the information will be protected from disclosure without their consent. The complaint alleged that material security deficiencies and lack of safeguards were noted in repeated audits posing "a significant threat to its systems," and were not corrected. Among the alleged deficiencies, were lack of multi-factor identification to gain access to sensitive data, failure to terminate remote logged in sessions when employees were working out of the office, failure to encrypt sensitive data and failure to adequately train its employees "in electronic security techniques, defenses and protocols."

In sum, these cases demonstrate that the essence of the claims – whether sounding in tort, contract or statutory violation – target purported failures to exercise due care to implement the necessary safeguards in line with published standards to protect the

employees' PII. Plaintiffs' counsels have the benefit of hindsight, which is always perfect.

WHAT SHOULD EMPLOYERS DO?

So what should employers, and in particular their legal and human resources departments, without the benefit of hindsight, do in the first instance to protect their companies against these risks? The strategy should be to take precautionary personnel and other measures in line with accepted standards for protecting employee PII (e.g., NIST standards) grounded in the lessons gleaned from the above cases. The focus should be both as to employee PII at rest and in transit. The following steps should be followed:

- As to sensitive employee PII normally maintained by personnel departments (e.g., benefits information, family and medical leave requests, medical information, tax information, social security numbers, disability related information, addresses, insurance information, direct deposit and banking information, birthdates, drivers' license information) the company should identify where the data is maintained on its electronic systems, who has access and how access is obtained. This is a comprehensive analysis of personnel software and systems, including servers, individual desktops, laptops and mobile devices, to document where this information is maintained.

- The company should determine the likelihood that a particular threat will exploit a particular vulnerability to gain unauthorized access to the employee PII and the resulting business impact. A threat analysis should assess not only the impact from a potential breach of confidentiality (e.g., identity theft), but also lack of availability (e.g., a hacker may encrypt the company's personnel/payroll information with ransomware and not release it until the demanded monies are paid).

- Steps should be taken to identify and address any gaps in protections to these threats for the stored employee PII (e.g., encryption, limiting access to Human Resources personnel, strong passwords, etc.).

- There should be personnel policies regarding the dissemination of confidential employee information using the company's electronic systems. For example, human resources should ensure that there are policies and procedures requiring sending employee tax related and other confidential information by email only if there is 100 percent confidence that the intended recipient is within the organization and has requested the information. Indeed, the IRS advises that employers consider adopting written policies that govern the electronic distribution of confidential employee Form W-2s and tax related information.[18] One simple protective measure may be requiring a phone call confirmation before hitting the send button.

- In addition to procedures verifying that the recipient of sensitive PII is actually within the organization, employers should consider technologies and policies providing for use of encryption when sending personnel related PII by email or storing it, particularly on laptops or portable media. As a general matter, employers should have in place comprehensive written policies and procedures that govern the electronic sending, receiving and storage of confidential personnel related PII.

- Employers should also consider implementing available tools to reduce risks from their own employees (such as comprehensive background checks and electronic system/email monitoring of those employees with access to employee PII) consistent with applicable laws.

- The risks from employees bringing personal devices to work ("BYOD") and the "Internet of Things" (and resulting risks from wireless connectivity) should also be addressed, including through personnel policies regulating the types of devices that can be worn or used in the workplace. The uncertainty around whether these devices are secure creates a known risk that employers should be addressing in their personnel and other electronic use policies.[19]

- Once the personnel policies and technologies are in place, training is very important both in preventing breach and in defending against claims should a breach occur. Most human resources departments are in various stages of identifying and scheduling their 2017-2018 compliance training schedule. Employers should prepare their workforce to protect employee and important organizational data from cyber threats.

Human resources departments already have in place the existing training, for example, the proper use of company technology and codes of conduct, to which specific training in cyber threats is a natural fit. Indeed, the proper use of the company's email system can include education and training on guarding against spearfishing and other social engineering attacks – one of the highest vulnerabilities. In addition, human resource's mission is to know its workforce and personnel, so it is well equipped to take complex concepts and break them down to digestible nuggets of information, disseminate the information across the workforce, track the training, and provide follow up. Human resources can help their information technology professionals identify and avoid "real world" ways that employees may utilize "work arounds" to avoid IT's well-intentioned security and policy protocols (e.g., logging in as a coworker or not using a secure Virtual Private Network ("VPN") to remotely and securely send confidential information while traveling on business or working remotely from home). Human resources is well equipped to impress upon employees that they are the best defense to protect the company and their colleagues from harm. On the other hand, failure to follow proper procedures may result in job-related disciplinary action.

Lastly, employers should plan for a breach involving employee PII. Policies and procedures should be in place for responding to and investigating a breach of each system where PII is maintained. The written plan should be in place prior to breach, and

not be a reactive measure formulated ad hoc under the stress of a breach. It should include instructions, including to human resources and employee benefits personnel, and set responsibilities for the various stages of the response.

CONCLUSION

A well thought out strategy implementing a safety net of technologies, policies and training is the best defense to mitigate the risks that are causing general counsels to lose sleep at night.

Endnotes

[1] BDO Consulting's *Inside E-Discovery & Beyond: E-Discovery Complexities Driving Change* survey (Jan. 2017).

[2] TerraLex's *The General Counsel Excellent Report 2015* survey (2015).

[3] Ponemon Institute's *2016 Cost of Data Breach Study: United States* (June 2016).

[4] *See*, *e.g.*, 45 C.F.R. § 164.400-414 (requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information); N.Y. Gen. Bus. Law § 899-aa ("Any person or business which conducts business in New York State, and which owns or licenses computerized data which includes private information [unencrypted or for which the encryption key was acquired] shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization."); Mich. Comp. Law § 445.72 ("Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach… shall provide a notice of the security breach to each resident of this state…"); N.J. Stat. § 56:8-163 (requiring businesses holding personal information to provide notifications when a data breach occurs); Wash. Rev. Code § 19.255.10 (requiring notification of breach of security system containing personal information).

[5] Jim Finkle and Dan Burns, *St. Jude Stock Shorted On Heart Device Hacking Fears; Shares Drop*, Reuters, Aug. 25, 2016.

[6] St. Jude brought a defamation lawsuit against Muddy Waters Consulting LLC after it purportedly identified and published alleged wireless vulnerabilities in St. Jude's implantable cardiac rhythm devices claiming that hackers can seize control of the devices while engaged in short selling St. Jude's stock. *St. Jude Med., Inc. v. Muddy Waters Consulting, LLC*, No. 16-Civ. 030002 (DWF/JSM) (D. Minn. 2016)

[7] *See, e.g.*, FBI and NCCIC's Joint Analysis Report, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, JAR-16-20296A, December 29, 2016..

[8] *See, e.g., Enslin v. Coca-Cola Company et. al.* – Complaint – Class Action – No. 14-CV-06476-JFL (E.D. Pa. 2014); *see also In re: Target Corp. Customer Data Sec. Breach Litig. – Financial Institution Cases*, MDL No. 14-2522 (PAM/JJK) (No. 261) (D. Minn. Dec. 2, 2014) (in connection with complaint by financial institutions, court refused to dismiss negligence claims finding that assertions that Target purposely disabled security features that would have prevented the breach and failed to heed the warning signs as the attackers' attack began creating a foreseeable risk of harm plausibly pled a general negligence case).

[9] *See, e.g.,* Cal. Civil Code § 56.20(a) ("Each employer who receives medical information shall establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information."), § 56.36(b) ("an individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her in violation of this part . . ."). As explained by the California courts, the term "released" does not connote an affirmative act on the part of the employer. *Regents of the Univ. of California v. Superior Court*, 220 Cal. App. 4th 549, 564-65 (Cal. Ct. App. 2013), *modified*, 2013 Cal. App. LEXIS 917 (Cal. Ct. App. Nov. 13, 2013) (where an employer negligently maintains confidential medical information, thereby allowing an unauthorized third person to access it, the employer may have negligently "released" the information within the meaning of the CMIA); Mich. Comp. Law § 445.86 (providing private cause of action for release of social security numbers).

[10] *See*, e.g., N.Y. Gen. Bus. Law § 899-aa (authorizing attorney general action); Mich. Comp. Law § 445.72 (authorizing attorney general action).

[11] *See In re Target Corp. Data Sec. Breach Litig. – Consumer Cases*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (finding that plaintiffs had standing to sue when theft of plaintiffs' identities caused them injuries that included unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees); *Cf. Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (in a case where defendant provided notice of breach to 27,000 employees within 30 days of breach, the court held that plaintiffs lacked any injury in fact for standing based on claims of increased risk of identity theft where no allegation that any theft had occurred as "hypothetical future" allegations do not establish standing); *see also Clapper v. Amnesty Int'l*, 133 S. Ct. 1138, 1160 (2013) (Article III standing requires the risk of future harm to be "certainly impending."); *In re SAIC Backup Tape Data Theft Litig.*, MDL No. 2360 (D.D.C. May 9, 2014) (loss of data without evidence of misuse is insufficient to establish standing). It would indeed be a thin reed, however, for an employer to failure to adequately institute protective measures in reliance on legal defenses that may (or may not) be later available if a lawsuit results from a breach of employee PII (*e.g.*, lack of standing, economic loss doctrine). *See*, *e.g.*, *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 3:16-cv-00014-GPC-BLM, 2016 U.S. Dist. LEXIS 152838, at *8 (S.D. Cal. November 3, 2016) ("[i]njury-in-fact analysis is highly case specific.").

[12] *Enslin v. Coca-Cola Company et. al.* – Complaint – Class Action – No. 14-CV-06476-JFL (alleging that the data stolen including social security numbers, drivers license records, personal addresses, and other data collected and maintained by Coke's human resources departments).

[13] *Enslin v. Coca Cola Company et. al.* – Decision, No. 14-CV-006476-JFL (E. D. Pa. Sept. 29, 2015) (dismissing negligence claim because plaintiffs asserted only the existence of standard employment contract, and did not allege any fiduciary duty or reliance on employer's expertise).

[14] *See, e.g., Leibovic v. United Shore Mort*., LLC, No. 15-12639 (E.D. Mich. Oct. 28, 2016) (refusing to dismiss common law negligence claim where plaintiff consumer alleged duty arose from defendants' acceptance of PII).

[15] *Enslin.* – Decision, No. 14-civ.-006476-JFL.

[16] *Corona v. Sony Pictures Entm't, Inc.*, Case No. 2:14-cv-09600 (C.D. Ca. June 15, 2015).

[17] *In Re U.S. Office of Personnel Management Data Security Breach Litigation*, 15-Civ.-1394 (ABJ) (D.D.C. March 14, 2016) (complaint). Defendants made a motion to dismiss which was pending as of March 1, 2017.

[18] *See* IRS February 2017 phishing alert.

[19] *See*, *e.g.*, Peterson, A., *"'Internet of Things'" compounded Friday's hack of major websites*, The Washington Post, Oct. 21, 2016.